基于 DNA 编码和超混沌系统的图像加密算法 *

张勋才，刘奕杉，崔光照

(郑州轻工业学院 电气信息工程学院，郑州 450002)

摘　要：针对 DNA 编码规则单一和混沌加密算法对密钥的灵敏度低等问题。提出一种基于 DNA 编码和超混沌系统的图像加密方案。该算法首先使用 SHA-3 算法计算明文图像的哈希值，用于超混沌系统的初始值，增加明文敏感性；其次将图像转换为 DNA 序列，并与所构建的 S 盒子进行 DNA 序列运算；最后用超混沌系统产生的序列对图像进行置乱。结果和理论分析表明，该算法不仅提高了密钥敏感性和传输数据的安全性，而且具有较好的抗穷举攻击、统计攻击和差分攻击能力。

关键词：图像加密；DNA 编码；超混沌系统；S 盒子；SHA-3

中图分类号：TP309.7　　doi: 10.3969/j.issn.1001-3695.2017.10.0997

Image encryption algorithm based on DNA encoding and hyper-chaotic system

Zhang Xuncai, Liu Yishan, Cui Guangzhao

(*College of Electrical & Information Engineering*, *Zhengzhou University of Light Industry*, *Zhengzhou* 450002, *China*)

Abstract: Aiming at the deficiency of the single DNA encoding rule and chaotic encryption algorithm has low sensitivity to key. This paer proposed an image encryption algorithm based on DNA encoding and hyper-chaotic system. Firstly, the algorithm used the SHA-3 algorithm to calculate the hash value of the plaintext image, which used for the initial value of the hyper-chaotic system and increases the sensitivity of plaintext. Secondly, the it converted image into DNA sequence and performed the DNA sequence operation with the constructed S-box. Finally, it scrambled the image by the sequence produced by hyper-chaotic system. The simulation results and theoretical analysis show that the algorithm improves the sensitivity of key and the security of data transmission, and has better ability of anti-exhaustive attack, statistical attack and differential attack.

Key Words: image encryption; DNA encoding; hyper-chaotic system; S-box; SHA-3

0　引言

近年来图像传输在医学影像、在线教学、通信等各个领域中被广泛使用。然而网络的开放性和共享性使得图像传输的安全性遭到巨大威胁。2013 年的“棱镜门”事件让人们意识到解决信息安全传输问题刻不容缓。图像加密技术是保护图像安全传输的一种有效方案。由于图像具有高冗余度、大数据容量、像素之间相关性强等特点，所以图像加密需要使用快速的算法[1~4]。传统的加密方法，如 DES、AES 和 RSA 等已经不能满足当前的图像加密。

近年来学者们提出了一些新的图像加密算法，如基于混沌理论的图像加密方法[5~8]和基于 DNA 序列的图像加密方法[9]。混沌系统具有良好的伪随机特性、轨道的不可预测性、对初始状态及控制参数的敏感性等一系列特性。这些特性与密码学的很多要求是吻合的。也正因为混沌与密码学之间有着密切的联系，所以混沌密码学得到了大量的研究，并应用于图像的加密中[10,11]。但是低维混沌系统产生的混沌只可短期预测，混沌序列随机性往往较差，加密图像密钥空间小，安全性能低，易于破译[12,13]。为扩大密钥空间和增加混沌序列的随机性，学者们设计了基于超混沌[14,5]、多级混沌[16,17]等图像加密算法。目前超混沌已广泛应用于非线性电路、安全通信、激光、神经网络、生物系统等领域。但随着密码分析技术的提高，超混沌加密技术也暴露出了对密钥的低敏感性等问题。

DNA 分子所固有的超大规模并行性、超低的能量消耗和超高的存储密度，使得基于 DNA 计算的图像加密算法具有传统密码算法所不具有的独特优势[18~20]。因为生物实验耗费巨大，Ning 等人提出一种伪 DNA 加密方法。该方法利用 DNA 计算中所涉及的基本思想，在电子计算机上模拟信息加密，但该方法不太适用于图像加密。2010 年薛等人提出了一种基于 DNA 编码与混沌序列相结合的加密方法。该方法利用 DNA 编码和

基金项目：国家自然科学基金资助项目（61602424，61472371，61472372，61572446）；河南省科技创新人才计划资助项目（174100510009）；河南省高等学校重点科研项目（18A510020）

作者简介：张勋才（1981-），男，河南周口人，副教授，博士，主要研究方向为智能信息处理、信息安全（zhangxuncai@pku.edu.cn）；刘奕杉（1992-），女，硕士研究生；主要研究方向为生物信息处理、信息安全；崔光照（1957-），男，教授，博士，主要研究方向为生物信息处理、信息安全.

超混沌系统对初始条件的敏感性和高度随机性提供了很好的加密效果。文献［21］提出一种基于混沌和 DNA 动态编码的图像加密算法，该算法加入了动态 DNA 编码规则，但是加密过程中 DNA 运算规则单一。文献［22］提出一种基于 DNA 序列的彩色图像加密算法，该算法在位平面进行 DNA 编码，但是编码与解码方式单一。文献[23]指出采用固定编码和单一运算规则的 DNA 混沌图像加密算法容易通过选择明文攻击进行破解。文献[24~26]提出了改进的基于编码和多混沌映射的图像加密算法，用超混沌系统置乱像素位置和像素值，用 DNA 编码规则编码进行伪 DNA 运算，最后通过 DNA 解码获得加密图像。文献[27]指出当前基于 DNA 编码和混沌理论对真彩图的加密算法对明文攻击的脆弱性，加密算法中存在对明文的低敏感性和对密钥的低敏感性等不足之处。文献[28]研究发现当算法加密过程与明文无关时，算法无法有效抵抗已知明文和选择明文攻击。

为此，本文结合超混沌系统、DNA 计算和哈希函数对图像进行分块加密，使用哈希函数 SHA-3 对原图像进行处理，进而获得超混沌系统的初始值以及与原图像异或的图像矩阵，将原图像与密钥的获得联系在一起，再利用超混沌系统产生的超混沌序列值，构造 S 盒子，使用 S 盒子对图像进行加、减和移位等操作。该算法不仅能有效提高密钥敏感性、传输数据的安全性，还能有效地抵抗已知明文和选择明文攻击，而且具有较好的抗穷举攻击、统计攻击和差分攻击能力等。

1 混沌系统与 DNA 编码

1.1 超混沌 LÜ 系统

2005 年，文献[29]给出了超混沌吕系统的详细描述：

$$\begin{cases} \dot{x} = a(y-x)+u \\ \dot{y} = -xz+cy \\ \dot{z} = xy-bz \\ \dot{u} = xz+du \end{cases} \tag{1}$$

其中：参数 a、b、c 为吕系统的参数；参数 d 是待定的控制增益参数；x、y、z、u 是变量。当 a=36，b=3，c=20，-0.35<d≤1.3 时，上述系统处于超混沌状态。

1.2 DNA 编码与运算

1)DNA 编码

DNA 是一种由脱氧核糖核酸作为基本单位的高分子聚合物。而脱氧核苷酸则是由三部分组成，分别为一分子的磷酸、一分子的脱氧核糖和一分子的含氮碱基。含氮碱基共有四种类型，即腺嘌呤(A)、胞嘧啶(C)、鸟嘌呤(G)、胸腺嘧啶(T)。其中 A 与 T、G 与 C 分别是两两互补的关系[30]。灰度图像的每一个像素可用 8 位二进制数表示，而二进制数中 0 和 1 互补，所以 00 和 11、01 和 l0 也是分别互补的。因此，如果用四个脱氧核苷酸 A、T、C、G 分别表示二进制数 00、11、01、10，则每一个像素值就可以用长度为 4 的 DNA 序列来表示。例如十进制值 200 表示为$(11001000)_2$，被转换为 4 位 DNA 序列是 TAGA。满足 DNA 碱基之间互补关系的编码规则有八种，如表 1 所示。

表 1 八种 DNA 编码规则

规则 1	规则 2	规则 3	规则 4	规则 5	规则 6	规则 7	规则 8
00-A	00-A	00-C	00-C	00-T	00-T	00-G	00-G
01-C	01-G	01-T	01-A	01-C	01-G	01-A	01-T
11-T	11-T	11-G	11-G	11-A	11-A	11-C	11-C
10-G	10-C	10-A	10-T	10-G	10-C	10-T	10-A

2)DNA 序列的运算

DNA 序列的加减法类似于传统的代数计算。当用 00-A、11-T、01-C、10-G 进行编码时，碱基之间的加减法运算规则如表 2 所示。

表 2 DNA 加减法则

+	A	T	C	G	-	A	T	C	G
A	A	T	C	G	A	A	T	C	G
T	T	A	G	C	T	T	T	A	C
C	C	G	A	T	C	C	C	G	T
G	G	C	T	A	G	G	G	C	A

2 方案设计

通过采用超混沌系统、DNA 编码和哈希函数对图像进行混淆和置乱来实现对图像的加密。

2.1 对角线提取法

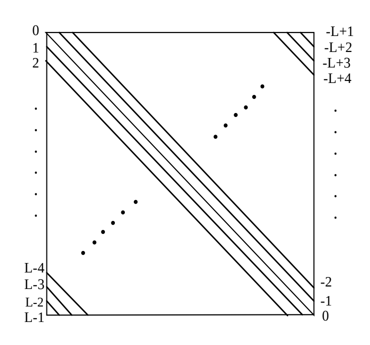


图 1 对角线示意图

对于大小为 $L*L$ 的原始灰度图像(在此默认灰度图像为方阵图像，若加密图像不是方阵，则进行填补，填补规则在后面叙述)，定义图像的主对角线为 diag(0)，主对角线以上平行于对角线每条线段依次定义为 diag(-1)，diag(-2)，…，diag($-L+1$)；主对角以下平行于对角线的每条线定义为 diag(1)，diag(2)，...，diag(L-1)。定义方式如图 1 所示。

为了达到置乱的效果，本文重新组合像素的位置。从图中提取像素的规则如下：

$$X_i = \text{diag}(i)+\text{diag}(-L+i) \tag{2}$$

其中：i=0，1，2，....，L-1。

举例：当 i=0 时，X_0=diag(0)+diag(-L)=diag(0)；X_1=diag(1)+diag(-L+1)。

按此方法，将每次提取出的 L 个元素分别转换成 $\sqrt{L}*\sqrt{L}$

的图像子矩阵，由此将得到 L 个 $\sqrt{L}*\sqrt{L}$ 的图像子矩阵。

2.2　SHA-3 算法

SHA-3 算法基于海绵结构[31]，是现代密码学中最基本的模块之一，以任意长度的消息值作为输入，都将生成固定长度的 HASH 值。由哈希值产生的密钥，即使原图像有极其微小的变化，都将产生一个完全不同的加密密钥。因此这种加密方法能有效地抵抗蛮力攻击。

原始图像用 SHA-3 转换后，将产生出一组 256 位的哈希值：dbbf374d57de108723c923b41d768d018c8e538a2de7479962c487a0335e1e85；将生成的哈希值作为下次哈希函数的输入信息来产生新的哈希值。循环产生八次，共得到 256*8 位哈希值。选择一种 DNA 编码规则对所得到的哈希值进行编码，每 8 位哈希值一组进行编码，将 256*8 位哈希值编码后转换为 16*16 的 DNA 编码矩阵。比如按第一种编码规则：db→11011011→TCGT。

2.3　密钥的产生

利用 SHA-3 产生的第一组哈希值作为密钥 K，用于产生混沌系统的初始值。将 K 按字节划分，可表示为 k_1，k_2，k_3，…，k_{32}。通过式(3~6)来计算混沌系统的初始值。

$$x_1=(k_1\oplus k_2\oplus.....\oplus k_8)/4+x_0 \quad (3)$$

$$y_1=(k_8\oplus k_9\oplus.....\oplus k_{16})/4 \quad (4)$$

$$z_1=(k_{16}\oplus k_{17}\oplus.....\oplus k_{24})/4 \quad (5)$$

$$u_1=(k_{24}\oplus k_{25}\oplus.....\oplus k_{32})/4 \quad (6)$$

其中：x_1、y_1、z_1、u_1 为超混沌吕系统的初始值；x_0 位给定值。

通过这种方式生成的密钥具有良好的随机性、周期性以及长密钥空间性等优势。将原图像信息与密钥相结合，算法将有效抵抗已知明文和选择明文攻击。

2.4　S 盒子

设定超混沌吕系统中的控制参数 a=36，b=3，c=20，d=1，采用 2.3 节得到的初始值，用超混沌吕系统生成四组超混沌序列，并用生成的混沌序列构造 S 盒子。其步骤如下 ：

a)构造一个空序列 M。

b)将区间［0，256］划分成 256 个子区间[(0，1)，…，(j，j+1)，…，((255，256)]，并用 T_j 表示 j=(0，1，2…，255)，如图 2 所示。

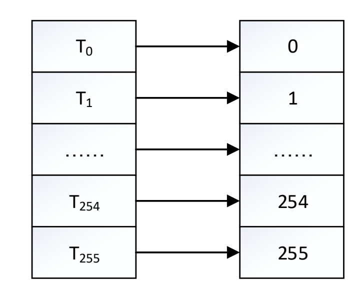


图 2　子区间与整数值之间的对应关系

c)超混沌吕系统迭代 i 次得到的状态值 x_i，y_i，z_i 和 u_i。通过式（7）~（10）对产生的混沌序列进行预处理，得到最终值 $f(x_i)$、$f(y_i)$、$f(z_i)$、$f(u_i)$。

$$f(x_i)=\mathrm{mod}(x(i)*1000，255) \quad (7)$$

$$f(y_i)=\mathrm{mod}(y(i)*1000，255) \quad (8)$$

$$f(z_i)=\mathrm{mod}(z(i)*1000，255) \quad (9)$$

$$f(u_i)=\mathrm{mod}(u(i)*1000，255) \quad (10)$$

d)若 $f(x_i)$位于第 j 个子区间(j，j+1)，且 j 不存在于序列 M 中，则在序列 M 中加上 j，其他依此类推。

e)如果在序列 M 中的元素个数小于 256，继续步骤 c)和 d)，直到序列 M 中的元素个数为 256。

f)将序列 M 中的 256 个元素转换成 16*16 的矩阵，得到一个 16*16 的 S 盒子。依照这种方法构造 16 个 16*16 的 S 盒子，并进行顺序编码。例如，通过初始值迭代超混沌吕系统生成的值 233.6，这个值位于子区间于 233~234 中，属于 T_{233}。若 233 不在序列 M 中，则把该值添加到序列 M 中，并进行 DNA 编码。

2.5　加密方案

该加密算法主要内容是首先将原始图像按 2.1 节所示的提取规则分割成 L 个子图像矩阵，其次将 SHA-3 算法产生的哈希值编码后与 DNA 编码过的子图像矩阵进行 DNA 编码运算，最后用超混沌吕系统生成的序列值所构造的 S 盒子对图像进行置换与置乱等加密。加密流程如图 3 所示。具体步骤如下：

a)输入 8 位灰度图像 I(m，n)。将图像按以下规则进行补图得到图像 I'（L，L）：

$$L=\max(\lfloor(\sqrt{m})^2\rfloor,\lfloor(\sqrt{n})^2\rfloor) \quad (11)$$

其中：$\lfloor(\sqrt{m})^2\rfloor$为$\lfloor(\sqrt{m})^2\rfloor$上取整。

b)将图像依照 2.1 节所示方法转换成 L 个 $\sqrt{L}*\sqrt{L}$ 的图像子矩阵。

c)对图像子矩阵的每个元素进行 DNA 编码。

d)将通过 2.2 节得到的大小为 16*16 的 DNA 编码矩阵，与步骤 c)中得到的 L 个图像子矩阵根据表 2 中的规则进行 DNA 序列运算。

e)用 2.4 节中构造的 16 个 S 盒子与步骤 d)中所得的 L 个图像子矩阵根据表 2 中的规则进行 DNA 编码运算。再对进行运算后的 L 个图像子矩阵进行左循环移 3 位加密操作（根据多次实验，循环移 3 位效果最佳。）

f)提取超混沌序列 $f(x_i)$、$f(y_i)$的前 1/2 的奇数位相加，序列 $f(z_i)$、$f(u_i)$的前 1/2 的偶数位相加组合成新的混沌序列 G，对该混沌序列取模 256，顺序提取该序列的 L 个数，提取 L 组，分别为 G_1、G_2…G_L，将每组 L 个数转换为 $\sqrt{L}*\sqrt{L}$ 的矩阵，将 L 个矩阵转换为二进制并选择一种 DNA 编码规则进行编码，再与步骤 e)所得的 L 个 $\sqrt{L}*\sqrt{L}$ 图像子矩阵根据表 2 中的 DNA 编码运算规则进行运算。

g)将步骤 f)所得的 L 个图像子矩阵合成一个图像矩阵 I_1。

h)根据式(12)产生的矩阵 C，将矩阵 I_1 与 C 根据表 2 中的

规则进行 DNA 序列运算，得到一个图像矩阵 I_2。

$$C= L *L*(x(L+j)+0.5))*ones(L,1) \tag{12}$$

其中:j= 1，2，3，…，256。

i)提取超混沌序列 $f(x_i)$、$f(y_i)$前 1/2 的偶数位相加，序列 $f(z_i)$、$f(u_i)$前 1/2 的奇数位相加组合成新的混沌序列 G_0，按从小到大的顺序排列，得到新序列，用新序列各元素所在的位置之值替换原序列中的该元素，得到新序列的索引，用新序列索引对图像矩阵 I_2 进行置乱，得到图像 I_3。

j)对图像 I_3 进行 DNA 解码，得到加密图像 I_4。

解密算法是加密算法的逆过程。在此不再详述。

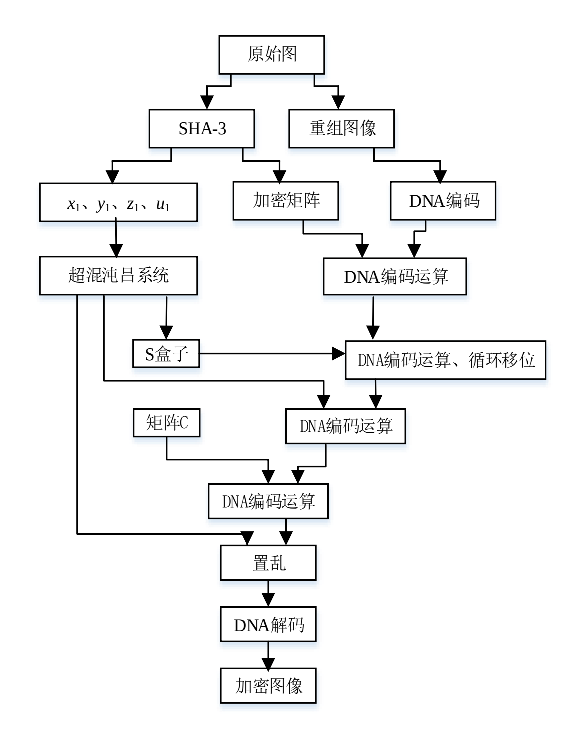


图 3　加密流程

3　仿真实验

在 MATLAB 7.1 环境下对本文提出的算法进行仿真。原始图像采用标准的 256*256 的 Lena 灰度图像，在 x_0=1 的条件下，该算法的实验结果如图 4 所示。



（a）原始图像　　(b)加密图像

图 4　图像加密、还原前后对比

4　安全性分析

算法的安全性分析主要包括密钥空间、灵敏性分析及抗统计攻击分析等。

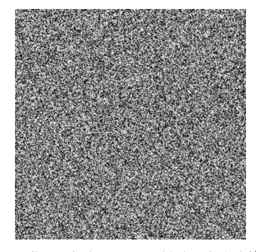
4.1　穷举攻击分析

1)密钥空间分析

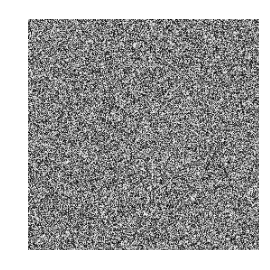
在本算法中，密钥包含：x_1、y_1、z_1、u_1、SHA-3 函数的 256 个字节。如果 x_1、y_1、z_1、u_1 的计算精度为 10^{14}，吕系统的密钥空间为 $10^{14}\times10^{14}\times10^{14}\times10^{14}=10^{56}$，SHA-3 的密钥空间为 2^{128}。总的密钥空间为 $10^{56}\times2^{128}\approx3.4\times10^{94}$ 可见该算法具有足够大的密钥空间来抵抗穷举攻击。

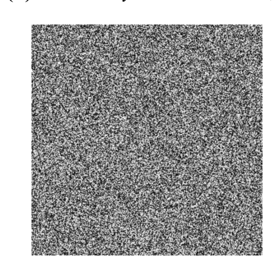
2)密钥的灵敏度分析

为测试密钥的灵敏性，用微小差异的密钥进行解密。图 5(a)表示 x_1=3 其他密钥不变的解密图；(b)~(d)分别表示 y_1=10，z_1=30，u_1=2 其他密钥不变的解密图。只要密钥有的小差异，原始图像将不能正确解密，且错误解密图像不能反映原始图像的信息。因此，可以得到该算法具有密钥的敏感性，并能有效抵抗暴力攻击。



(a)错误密钥 x_1=3 的解密图像　　(b)错误密钥 y_1=10 的解密图像





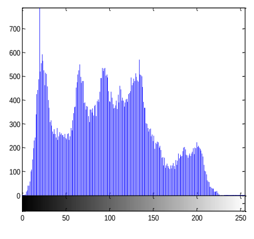
(c)错误密钥 z_1=30 的解密图像　　(d)错误密钥 u_1=2 的解密图像

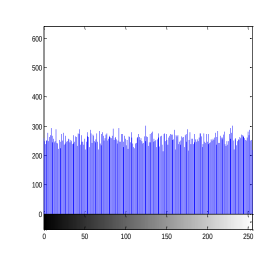
图 5　错误密钥下的解密图像

4.2　统计攻击分析

1)直方图分析

对于原始图像和加密图像的统计分析，分析其统计特性。图 6(a)给出了原始图像直方图，(b)给出了加密图像直方图。原始图像象素值比较集中，而加密图像的直方图基本上是均匀的，攻击者难以利用像素灰度值的统计特性恢复原图像。由此可见该算法具有很好的抗统计分析能力。





(a)Lena 明文图像的直方图　　(b) Lena 密文图像的直方图

图 6　灰度直方图分析

2)相关性分析

从原始图像和加密图像中随机的选取在水平方向、垂直方向以及对角方向上 2 500 对相邻像素点，然后利用式(13~16)计算像素间的相关性。

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i \tag{13}$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2 \tag{14}$$

$$COV(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(x)) \tag{15}$$

$$r_{xy}=\frac{COV(x,y)}{\sqrt{D(x)}\times\sqrt{D(y)}} \tag{16}$$

其中：x 和 y 是图像中相邻像素的灰度值；cov(x, y)是协方差；$D(x)$是方差；$E(x)$是平均值。类似地，其他结果如表 3 所示。图 7 显示了原始图像和加密图像水平方向、垂直方向、对角线方向相邻像素的相关性。加密图像的相邻像素的相关系数为-0.0005348。因此，该图像加密算法具有较强的抗统计攻击能力。

表 3　原始图像和加密图像中两个相邻像素相关系数对比

相关系数	原始图像	加密图像
水平	0.9684	-0.0060
垂直	0.9394	-0.0038
对角线	0.9172	-0.0033

3)信息熵

信息熵被定义为描述系统的不确定性的程度，可以用来表示图像信息的不确定性。图像灰度值分布越均匀，其信息熵越大。其公式如下：

$$H(m)=-\sum_{t=0}^{t}P(m_i)\log_2 P(m_i) \tag{17}$$

$P(m_i)$是信息 m_i 出现的概率。对于灰度图像来说，信息 m 有 256 种状态，最小值 0，最大值为 255。一个理想的随机图像，信息熵的值是 8。实验的信息熵 7.989 7，说明该加密算法的有效性。

4.3　差分攻击分析

差分攻击是指攻击者通过对明文稍微改变，比较相应密文改变前后的差异，然后找出相应明文图像和密文图像的关系。通常采用 NPCR(像素改变率)和 UACI(像素平均改变强度)指标用来检测图像加密方案抵抗差分攻击的能力。采用下面的公式计算 NPCR 和 UACI：

$$NPCR=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}C(i,j)}{M\times N}\times 100\% \tag{18}$$

$$UACI=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left|P_1(i,j)-P_2(i,j)\right|}{255\times M\times N}\times 100\% \tag{19}$$

$$C(i,j)=\begin{cases}0, if\ P_1(i,j)=P_2(i,j)\\1, if\ P_1(i,j)\neq P_2(i,j)\end{cases} \tag{20}$$

其中：M 和 N 分别代表图像的长度和宽度；$P_1(i, j)$和 $P_2(i, j)$分别表示明文改变前后相对应的密文像素值。NPCR 值越接近于 100%，说明图像加密方案对明文图像敏感性越高，其抵抗差分攻击的能力越强。UACI 的理想值为 33%，其越接近于理想值，则说明抵抗差分攻击的能力也越强。

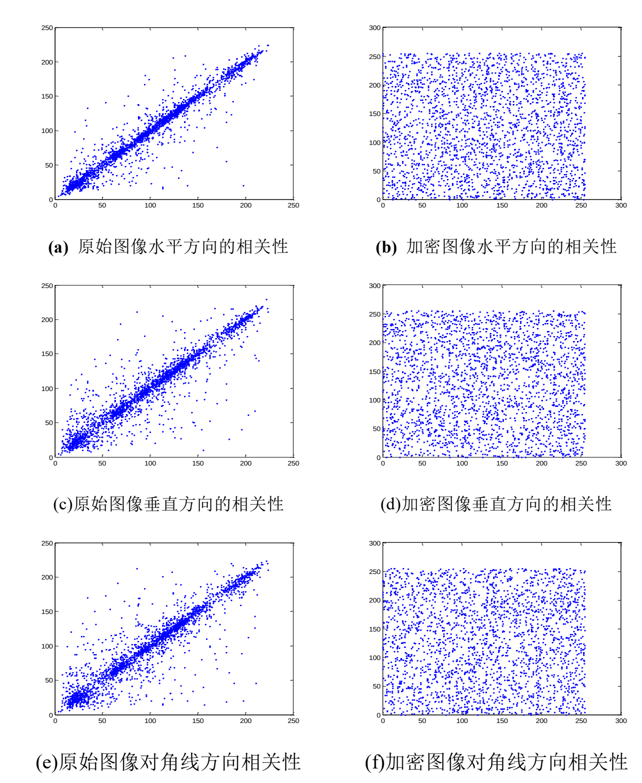


图 7　原始图像与加密图像在水平方向、垂直方向、对角线方向的两个相邻像素的相关性

改变明文图像中某一个像素值，如位置为(7，8)的像素值由 128 改为 30，然后根据上式可计算出 NPCR＝99.5956％，UACI＝33.39％。由此可见，NPCR 接近于 100%，并且 UACI 值也接近于 33%，这验证了该图像加密方案具有抵抗差分攻击的能力。

5　结束语

本文提出了一种基于 DNA 编码和超混沌相结合的图像加密算法，该算法通过采用 DNA 编码规则，并使用 SHA-3 算法提高了密钥空间；其次使用超混沌序列增加了本算法的复杂度和密文的不可预测性；最后 S 盒子的使用为本算法提供了双重安全性。实验分析表明，该算法不仅具有较好的加密效果，对密钥的敏感度较高；还可以有效抵抗穷举攻击、统计攻击和差分攻击。

参考文献：

[1] 朱淑芹，李俊青，王文宏. 对改进的基于 DNA 编码和混沌的图像加密算法的安全性分析 [J]. 计算机应用研究, 2017, 34 (10): 3090-3093.

[2] Van Droogenbroeck M. Partial encryption of images for real-time applications [C]// Proc of the 4th IEEE Signal Processing Symposium. 2004: 11-15.

[3] Seripeariu L, Frunza M D. A new image encryption algorithm based on inversable functions defined on galois fields [C]// Proc of IEEE International Symposium on Signals, Circuits and Systems. 2005: 243-246.

[4] Chen R J, Lai Y T, Lai J L. Architecture design of the re-configurable 2-D von neumann cellular automata for image encryption application [C]// Proc of IEEE International Symposium on Circuits and Systems. 2005: 3059-3062.

[5] Zhen W, Xia H, Yuxia L, et al. A new image encryption algorithm based on the fractional-order hyperchaotic Lorenz system [J]. Chinese Physics B, 2013, 22 (1) .

[6] Wang X, Teng L, Qin X. A novel colour image encryption algorithm based on chaos [J]. Signal Processing, 2012, 92 (4): 1101-1108.

[7] Guesmi R, Farah M A B, Kachouri A, et al. A novel chaos-based image encryption using DNA sequence operation and secure hash algorithm SHA-2 [J]. Nonlinear Dynamics, 2016, 83 (3): 1123-1136.

[8] Wang X, Wang X, Zhao J. Chaotic encryption algorithm based on alternant of stream cipher and block cipher [J]. Nonlinear Dynamics, 2011, 63, 587-597.

[9] Wei X, Guo L, Zhang Q, et al. A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system [J]. Journal of Systems and Software, 2012, 85 (2): 290-299.

[10] Zhang Y, Tang Y. A plaintext-related image encryption algorithm based on chaos [J]. Multimedia Tools and Applications, 2017: 1-23.

[11] Akhavan A, Samsudin A, Akhshani A. Cryptanalysis of an image encryption algorithm based on DNA encoding [J]. Optics & Laser Technology, 2017, 95: 94-99.

[12] Alvarez G, Montoya F, Romera M, et al. Cryptanalysis of an ergodic chaotic cipher [J]. Physics Letters A, 2003, 311 (2): 172-179.

[13] Elnashaie S, Abashar M E. On the chaotic behaviour of forced fluidized bed catalytic reactors [J]. Chaos, Solitons & Fractals, 1995, 5 (5): 797-831.

[14] Liu W, Sun K, Zhu C. A fast image encryption algorithm based on chaotic map [J]. Optics & Lasers in Engineering, 2016, 84: 26-36.

[15] 朱从旭，胡玉平，孙克辉. 基于超混沌系统和密文交错扩散的图像加密新算法 [J]. 电子与信息学报, 2012, 34 (7): 1735-1743.

[16] Gao Tiegang, Chen Zengqiang. A new image encryption algorithm based on hyper-chaos [J]. Physics Letters A, 2008, 372 (4): 394-400.

[17] Kumar M, Iqbal A, Kumar P. A new RGB image encryption algorithm based on DNA encoding and elliptic curve diffie–Hellman cryptography [J]. Signal Processing, 2016, 125: 187-202.

[18] Zhou C, Wei X, Zhang Q, et al. DNA sequence splicing with chaotic maps for image encryption [J]. Journal of Computational and Theoretical Nanoscience, 2010, 7 (10): 1904-1910.

[19] Wang Q, Zhang Q, Wei X. Image encryption algorithm based on DNA biological properties and chaotic sys-tems [C]// Proc of the 15th International Conference on Bio-Inspired Computing: Theories and Applications (BIC-TA) . 2010: 132-136.

[20] Adleman L. Molecular computation of solutions to combinatorial problems [J]. Science, 1994, 266 (5187): 1020-1024.

[21] 田海冰，雷鹏，王永. 基于混沌和 DNA 动态编码的图像加密算法 [J]. 吉林大学学报：工学版, 2014, 44 (3): 801-806.

[22] 涂正武，金聪. 基于DNA序列的彩色图像加密算法 [J]. 计算机工程与科学, 2015, 37 (10): 1933-1939.

[23] Özkaynak F, Yavuz S. Analysis and improvement of a novel imagefusion encryption algorithm based on DNA sequence operation andhyper-chaotic system [J]. Nonlinear Dynamics, 2014, 78 (2): 1311-1320.

[24] Özkaynak F, Özer A B, Yavuz S. Security analysis of an image encryption algorithm based on chaos and DNA encoding [C]// Proc of the 21st Signal Processing and Communications Applications Conference. 2013: 1-4.

[25] Zhang Q, Liu L, Wei X. Improved algorithm for image encryption based on DNA encoding and multi-chaotic maps [J]. AEU-International Journal of Electronics and Communications, 2014, 68 (3): 186-192.

[26] Kong L, Li L. A new image encryption algorithm based on chaos [C]// Proc of the 35th Chinese Control Conference. 2016: 4932-4937.

[27] Liu Y, Tang J, Xie T. Cryptanalyzing a RGB image encryption algorithm based on DNA encoding and chaos map [J]. Optics & Laser Technology, 2014, 60: 111-115.

[28] 刘金梅，丘水生，刘伟平. 基于超混沌系统的图像加密算法的安全性分析术 [J]. 计算机应用研究, 2010, 27 (3): 1042-1044.

[29] Chen A, Lu J, Lu J, et al. Generating hyperchaotic Lü attractor via state feedback control [J]. Physica A-statistical Mechanics and Its Applications, 2006: 364: 103-110.

[30] Shiu H, Ng K, Fang J, et al. Data hiding methods based upon DNA sequences [J]. Information Sciences, 2010, 180 (11): 2196-2208. Enayatifar R, Sadaei H J, Abdullah A H, et al. A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata [J]. Optics and Lasers in Engineering, 2015: 71: 33-41.